

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-224219

(43)Date of publication of application : 11.08.2000

(51)Int.Cl.

H04L 12/46

H04L 12/28

H04L 12/56

(21)Application number : 2000-012842

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(22)Date of filing : 21.01.2000

(72)Inventor : EDWARD B BORDEN
FRANKLIN A GRUBER

(30)Priority

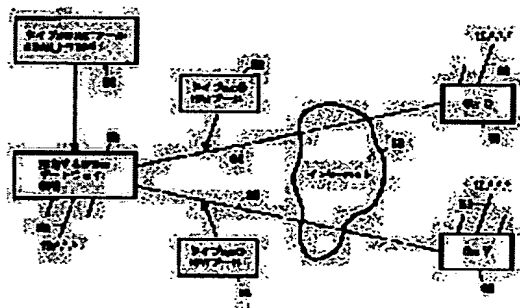
Priority number : 99 240720 Priority date : 29.01.1999 Priority country : US

(54) METHOD AND SYSTEM FOR OPERATING VIRTUAL PRIVATE NETWORK

(57)Abstract:

PROBLEM TO BE SOLVED: To make a NAT and an IP security compatible with each other by dynamically generating a network address transforming(NAT) rule and executing IP security in connection with security association.

SOLUTION: A user sets connection requiring the NAT and defines a pair of usable IP addresses among NAT pools 50, 52 and 54 to start mode connection. At the time of requiring transformation of a local client ID, a connection manager chooses a usable address from the NAT pools related with a remote ID, sends a start message to an ISAKMAP and loads connection to the IP security to generate a rule to SA. Next, mode connection on a responding side is started and SA is integrated based on prescribed policy to send as an SA aggregate formed of (n)-number of SA pairs. At the time of receiving a start message, a connection manager obtains an IP address from a proper NAT pool according to connecting definition and updates the SA pairs to finish connection.



LEGAL STATUS

[Date of request for examination] 21.01.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3393836

[Date of registration] 31.01.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11)特許番号

特許第3393836号

(P3393836)

(45)発行日 平成15年4月7日(2003.4.7)

(24)登録日 平成15年1月31日(2003.1.31)

(51)Int.Cl. ⁷	識別記号	P I
H 0 4 L 12/46		H 0 4 L 12/46 E
9/00		9/00
12/66		12/66 B

請求項の数17(全 13 頁)

(21)出願番号 特願2000-12842(P2000-12842)
(22)出願日 平成12年1月21日(2000.1.21)
(65)公開番号 特開2000-224219(P2000-224219A)
(43)公開日 平成12年8月11日(2000.8.11)
審査請求日 平成12年1月21日(2000.1.21)
(31)優先権主張番号 09/240720
(32)優先日 平成11年1月29日(1999.1.29)
(33)優先権主張国 米国 (US)

(73)特許権者 390009531
インターナショナル・ビジネス・マシー
ンズ・コーポレーション
INTERNATIONAL BUSI
NESS MACHINES COR
PORATION
アメリカ合衆国10504、ニューヨーク州
アーモンク ニュー オーチャード
ロード
(72)発明者 エドワード・ビー・ボーデン
アメリカ合衆国13850 ニューヨーク州
ベストル ナップ・ロード3217
(74)代理人 100086243
弁理士 坂口 博 (外1名)

審査官 中木 努

最終頁に続く

(54)【発明の名称】 仮想プライベート・ネットワークの動作方法およびシステム

(57)【特許請求の範囲】

【請求項1】 ネットワーク・アドレス変換 (NAT) を IP Sec処理と統合する IP Secに基づく仮想プライベート・ネットワーク (VPN) を動作させる方法であって、 NAT IPアドレス・プールを設定するステップと、前記 NAT IPアドレス・プールを使用するために VPN接続を設定するステップと、前記 NAT IPアドレス・プールから特定の IPアドレスを入手し、前記特定の IPアドレスを前記 VPN接続に割り振るステップと、前記 VPN接続を開始するステップと、オペレーティング・システム・カーネルに前記 VPN接続のためのセキュリティ・アソシエーションと接続フィルタをロードするステップと、前記 VPN接続のための IPデータグラムを処理するステッ

プと、
前記 IPデータグラムに VPN NATを適用するステップとを含む方法。

【請求項2】 前記 VPN接続が送出処理のために設定され、前記適用ステップが送出送信元 IPのネットワーク・アドレス変換を含む、請求項1に記載の方法。

【請求項3】 前記 VPN接続が到着処理の何らかの組合せのために設定され、前記適用ステップが到着送信元 IPのネットワーク・アドレス変換または到着宛先 IPのネットワーク・アドレス変換を選択的に含む、請求項1に記載の方法。

【請求項4】 手動鍵 IP Sec接続のための NATと IP Secとの統合のために、接続鍵を手動で設定するステップをさらに含む、請求項1に記載の方法。

【請求項5】 動的鍵 (たとえば IKE) IP Sec接続のため

3

のNATとIP Secとの統合のために、VPN接続の鍵を自動的に入手するように前記VPN接続を設定するステップをさらに含む、請求項1に記載の方法。

【請求項6】 NATをIKEによって動的にネゴシエーションされたIP Secセキュリティ・アソシエーションと統合するために、前記開始ステップが、前記NATプールからの前記IPアドレスを含むIKEのためにメッセージを作成するステップをさらに含み、動的にネゴシエーションされた鍵を入手するようにIKEを動作させるステップをさらに含む、請求項1に記載の方法。

【請求項7】 前記動的に入手した鍵を前記NATプールIPアドレスと結合するステップをさらに含み、前記ロードするステップが前記結果をセキュリティ・アソシエーションとして前記オペレーティング・システム・カーネルにロードするステップを含む、請求項6に記載の方法。

【請求項8】 VPN接続およびVPNポリシーの定義および設定を直接使用するNATの定義および設定を可能にする方法であって、

VPN NATタイプa 送出送信元IP NATとVPN NATタイプc 到着送信元IP NATとVPN NATタイプd 到着宛先IP NATの3つのタイプのVPN NATのうちの各タイプのためのポリシー・データベースにおける肯定/否定の決定によってVPN NATのための要件を設定するステップと、
前記各VPN NATタイプの前記肯定/否定の決定に回答してリモートIPアドレス・プールまたはサーバIPアドレス・プールを選択的に設定するステップとを含む方法。

【請求項9】 VPN接続が必要になる各リモート・アドレスのために固有な前記リモートIPアドレス・プールを設定するステップであって、前記リモートIPアドレス・プールがリモートIDによって鍵づけされるステップをさらに含む、請求項8に記載の方法。

【請求項10】 設定されるシステムのために1回前記サーバIPアドレス・プールを設定するステップをさらに含む、請求項8に記載の方法。

【請求項11】 VPN NATアドレス・プールをゲートウェイに関連づけることができるようにし、それによってサーバ負荷バランスをとることができるようにする方法であって、

設定するシステム用にサーバNAT IPアドレス・プールを設定するステップと、

前記サーバNAT IPアドレス・プールにグローバルにルーティング可能な特定のIPアドレスを格納するステップと、

前記サーバNAT IPアドレス・プールを使用するようにVPN接続を設定するステップと、

前記サーバNAT IPアドレス・プール内のアドレスの数に回答して、並列VPN接続の合計量を管理するステップとを含む方法。

【請求項12】 NATアドレスの可用性に基づいてシステムのためのVPN接続の合計数を制御する方法であって、

4

IPアドレスの共通セットを使用してリモートIPアドレス・プール全体を設定するステップと、
前記リモート・アドレス・プール全体にわたって設定された前記IPアドレスの数に回答して、並列してアクティブであるVPN接続の成功裏の開始を制限するステップとを含む方法。

【請求項13】 ネットワーク・アドレス変換(NAT)をIP Sec処理と統合するIP Secに基づく仮想プライベート・ネットワーク(VPN)を動作させるシステムであって、

NAT IPアドレス・プールを設定する手段と、
前記NAT IPアドレス・プールを使用するためにVPN接続を設定する手段と、

前記NAT IPアドレス・プールから特定のIPアドレスを入手し、前記特定のIPアドレスを前記VPN接続に割り振る手段と、

前記VPN接続を開始する手段と、

オペレーティング・システム・カーネルに前記VPN接続のためのセキュリティ・アソシエーションと接続フィルタをロードする手段と、

前記VPN接続のためのIPデータグラムを処理する手段と、

前記IPデータグラムにVPN NATを適用する手段とを含むシステム。

【請求項14】 VPN接続およびVPNポリシーの定義および設定を直接使用するNATの定義および設定のためのシステムであって、

VPN NATタイプa 送出送信元IP NATとVPN NATタイプc 到着送信元IP NATとVPN NATタイプd 到着宛先IP NATの3つのタイプのVPN NATのうちの各タイプのための肯定/否定の決定によってVPN NATのための要件を設定するポリシー・データベースと、

前記各VPN NATタイプの前記肯定/否定の決定に回答して選択的に設定されるリモートIPアドレス・プールまたはサーバIPアドレス・プールとを含むシステム。

【請求項15】 VPN NATアドレス・プールをゲートウェイに関連づけることができるようにし、それによってサーバ負荷バランスをとることができるようにするシステムであって、

設定される所与のシステム用に設定されたサーバNAT IPアドレス・プールと、

グローバルにルーティング可能な特定のIPアドレスを格納する前記サーバNAT IPアドレス・プールと、

前記サーバNAT IPアドレス・プールを使用するように設定されたVPN接続と、

前記サーバNAT IPアドレス・プール内のアドレスの数に回答して、並列VPN接続の合計量を管理する接続コントローラとを含むシステム。

【請求項16】 ネットワーク・アドレス変換(NAT)をIP Sec処理と統合するIP Secに基づく仮想プライベート

5

・ネットワーク (VPN) を動作させる方法ステップを実行するように機械によって実行可能な命令から成るプログラムを有形に実施する、機械による読取り可能なプログラム記憶装置であって、前記方法ステップは、
NAT IPアドレス・プールを設定するステップと、
前記NAT IPアドレス・プールを使用するためにVPN接続を設定するステップと、
前記NAT IPアドレス・プールから特定のIPアドレスを入手し、前記特定のIPアドレスを前記VPNに割り振るステップと、
前記VPN接続を開始するステップと、
オペレーティング・システム・カーネルに前記VPN接続のためのセキュリティ・アソシエーションと接続フィルタをロードするステップと、
前記VPN接続のためのIPデータグラムを処理するステップと、
前記IPデータグラムにVPN NATを適用するステップとを含むプログラム記憶装置。

【請求項17】 ネットワーク・アドレス変換 (NAT) を使用して仮想プライベート・ネットワークにIPセキュリティを設ける方法であって、
NAT規則を動的に生成し、前記NAT規則を、手動または動的に生成された (IKE) セキュリティ・アソシエーションに関連づけるステップと、その後で、
前記セキュリティ・アソシエーションを使用するIPセキュリティを開始するステップと、その次に、
送出データグラムおよび到着データグラムに対してIPSecが実行されるときに、VPN NATタイプa送出送信元IP NAT、VPN NATタイプc到着送信元IP NAT、およびVPN NATタイプd到着宛先IP NATのうちの1つまたは複数のタイプを選択的に実行するステップとを含む方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、仮想プライベート・ネットワーク (VPN) 接続のセキュリティに関する。より詳細には、本発明は、VPN NAT、またはネットワーク・アドレス変換 (NAT) プロトコルとIPセキュリティ (IPSec) プロトコルとの併用に関する。

【0002】

【従来の技術】 ネットワーク・アドレス変換 (NAT) は、インターネットやインターネットに接続する企業で広く使用されており、IPセキュリティの問題を生じさせる。実際に、NATはIPセキュリティ (IPSec) を破る。すなわち、NATは、「ロケータと端点識別子の両方としてのIPアドレスの意味論的オーバーロードを最終的に破る機能」である。その結果、2つのホストの間にNATシステムがある場合、その2つのホストはIPSec接続を確立することができない。その理由は2つある。

【0003】 第1に、2つのホスト間を流れる (IPSec接続のための) IPトラフィックには、AHまたはESPが適

6

用される。トンネル・モードでのESPに関しては、変換する必要があるIPアドレスはESPトンネルの内部にあり、暗号化される。したがって、NATには使用することができない。トランスポート・モードまたはトンネル・モードでのAHに関しては、変換する必要のあるIPアドレスはNATでは可視であるが、AH認証にそのIPアドレスが含まれる。したがって、IPアドレスを変更すると、IPSec接続のリモート・エンドでその認証が破られることになる。トランスポート・モードでのESPに関しては、ESPが認証と共に使用される場合であっても、IPアドレスはNATにとって使用可能である。しかし、IPアドレスが変更された場合、IPSec接続のリモート・エンドでの認証の失敗のために、IPSec接続は失敗する。

【0004】 第2に、IPSec接続のIPトラフィックを変換することができたとしても、IPSec接続は2つのホストのIPアドレスを含むセキュリティ・アソシエーションに基づいているため失敗することになる。これらは、復号化が行われるホスト上の到着IPSecを以下の三つ組みによって固有に判断しなければならないために、セキュリティ・アソシエーション・アーキテクチャにとって重要である。

【宛先IPアドレス、SPI、IPSecプロトコル】

たとえば、ホストAおよびWがあるとして、AからWに流れるトランスポート・モードでESPを使用してIPデータグラム (回線を流れるバイトの総称) にNATを適用するものとする。このパケットは、(トンネリングされない非暗号化テキストであった) IP送信元アドレスに依存しないため、Wに着信するとおそらく成功裏に復号化される。しかし、厳密に実施された場合、変更されたIP送信元アドレスにより (セキュリティ・アソシエーションをネゴシエーションするために使用されたアドレスではなかったために)、復号の後に行う必要がある到着SPD検査が失敗する。したがって、トランスポート・モードESPの場合であっても失敗する。

【0005】 単にNATとIPSecとを相互に両立できないようにすることは、当技術分野で求められる解決策ではない。NATは、グローバル・アドレス変更の隠蔽、アドレス使用の低減、ISPサポート負担の軽減、仮想ホストとしての負荷分散が可能など、多くの問題を解決するため、広く使用されている。しかし、NATは、現在、インターネットに配備されているセキュリティ統合にとって、最大の単一の脅威と見られている。これは常に「NAT問題」と言われており、アーキテクチャ上の根本的な問題である。しかし、レガシー・アプリケーションおよびサービス (たとえばIPバージョン4用に配備されたものなど) は、アプリケーションやサービスがIPバージョン6用に発展していく間も長く共存し続けるであろう。したがって、当技術分野では、少なくとも選択された状況で、NATとIPSecの共存を実現する必要性が高く、その実現のために重大な構成上の問題を生じさせないこと

が必要である。

【0006】2つのアドレス・ドメイン間のVPN接続は、接続される予定がない可能性が最も高い2つのドメインを直接接続するという影響があることがある。したがって、VPNの使用の増大により、アドレス競合が増大する可能性が高くなる。また、VPNは、NATを通過するときに、ネットワークの可視性を再定義し、アドレスの衝突を起こす可能性が高くなることもわかる。NATの背後の隠れた空間でのアドレス管理は、著しい負担になる。したがって、当技術分野ではこの負担を軽くする必要がある。

【0007】

【発明が解決しようとする課題】本発明の目的は、ネットワーク・アドレス変換(NAT)とIPセキュリティ(IPSec)の両方を並列して実現する改良されたシステムおよび方法を提供することである。

【0008】本発明の他の目的は、仮想プライベート・ネットワーク(VPN)の使用に固有のIPアドレス競合の可能性の増大を解決するシステムおよび方法を提供することである。

【0009】本発明の他の目的は、(高くつく代替策である)ドメインの再アドレス指定の必要なしに、VPNの使用を可能にするシステムおよび方法を提供することである。

【0010】本発明の他の目的は、ドメイン・ホストに変更を加える必要なしに、完全にIPSecゲートウェイだけで実現されるVPN NATのためのシステムおよび方法を提供することである。

【0011】本発明の他の目的は、各接続ドメインにおいてルーティングにまったく変更を加える必要がないか、またはわずかな変更しか必要としない、VPN NATのためのシステムおよび方法を提供することである。

【0012】本発明の他の目的は、設定が単純なVPN NATのためのシステムおよび方法を提供することである。

【0013】本発明の他の目的は、VPNによって生じるアドレス衝突問題の解決策を提供することである。

【0014】

【課題を解決するための手段】本発明によると、3つのタイプのVPN NAT(ネットワーク・アドレス変換)のうちの1つのタイプまたはそれらの組合せを実行することによって、ネットワーク・アドレス変換(NAT)を使用する仮想プライベート・ネットワークにおいてIPセキュリティが設けられる。これには、NAT規則を動的に生成し、それらを手動または動的生成(IKE)セキュリティ・アソシエーションと関連づけてから、このセキュリティ・アソシエーションを使用するIPセキュリティを開始する。次に、送出および到着データグラムに対してIPSecを実行し、NAT機能も実行する。

【0015】

【発明の実施の形態】本発明の好ましい実施形態による

と、VPN NATとプリファード(Prefex) IP Secの2つの機能によってNAT問題に対処する。

【0016】プリファード(Prefex) IP Secによると、HID規則およびMAP NAT規則(従来型NATとも呼ぶ)の意図しない使用による正常に機能しないIP Sec接続を防ぐため、従来型NAT中にAHまたはESPがないかを检查する。AHまたはESPヘッダを除くIPパケットに所与のNAT規則が適用されるとすれば、アドレス変換は行われない。これは到着NATと送出NATに適用される。したがって、(IP Sec用のVPN NATまたはIP Sec NATに対して)従来型NATの場合、IP Secが優先される。IP Secは従来型NATを無効にする。

【0017】NAT規則がロードされる時点ではIP Sec接続が競合するかどうかかわからないため(たとえば動的IP)、SLICにおける実際のNAT処理までこのような問題の検査を行うことができない。この規則のためにジャーナル機能がオンになっている場合、データグラムにNAT規則が適合するがIP Secのために行われなかったことをジャーナル項目で示すことによって、これらのアクションに対するユーザ可視性をもたせる。さらに、1従来型NAT規則当たりある程度の限定された数のオカレンスについて、これらのアクションのLIC情報ロギングを行うことができる。同様に、1オカレンス単位ではなく1接続単位のメッセージを、接続マネージャ・ジョブ・ログまたは接続ジャーナルに入れることができる。

【0018】VPN NATと呼ぶ本発明によると、NATをIP SecゲートウェイでIP Secと共に使用することができるようにするために、顧客はプライベート内部IPアドレスを保持し、IP Sec接続をIP Secゲートウェイで開始および終了させることによってアドレス衝突の増大が回避される。

【0019】本発明の好ましい実施形態によると、組込みNAT機能を使用して開始側モードと応答側モードの両方に仮想プライベート・ネットワーク(VPN)を設ける。適切な外部(NAT rhs) IPアドレスを使用してセキュリティ・アソシエーションをネゴシエーションし、IPSecへの接続ロードおよびSLICにおけるIPSec処理と同期して、生成されたNAT規則によって対応する内部(NAT lhs) IPアドレスのNATを行う。到着送信元IPアドレスを変換し、(到着時の宛先IPアドレスの対応する変換と共に)送出時の通常の送信元IPアドレスNATも行う。

【0020】図1を参照すると、VPN NATを実行する本発明の好ましい実施形態の方法は、ステップ20でNATを必要とする接続を設定するステップと、ステップ22でIPSec NATプールを定義するステップと、ステップ24で開始側モード接続を開始するステップと、ステップ26で応答側モード接続(これらの接続は一般に接続の他端で開始される)を開始するステップと、ステップ28でSA対の更新を処理するステップと、ステップ30で接続を終了するステップとを含む。(NATプールはIP

ドレスのセットである。) これらの各ステップについて以下に詳述する。

【0021】ステップ20で、ユーザはNATを必要とする接続を決定し、設定する。これは、論理的にはNAT規 *

*則の作成と等しい。これを行う際に考慮する4つの事例を表1に示す。

【表1】

表1:VPN NAT のタイプ

	IDci	IDcr
開始側モード	タイプ a.NAT 内部アドレス、送出時のIP送信元、到着時のIP宛先。	タイプ b.外部で定義されるため適用せず。
応答側モード	タイプ c.NAT外部アドレス、到着時IP送信元、送出時IP宛先。	タイプ d.NAT 内部アドレス、到着時IP宛先、送出時IP送信元。

【0022】たとえばIP Secポリシー・データベースにNATの特定のインスタンスを指定する場合、ユーザはたとえばチェックボックスでyes/noの決定を行う。応答側モードNATフラグIDciおよびIDcrは、接続定義の一部とすることができる。開始側モード・フラグは、「ローカル・クライアントID」(専用)に付随するユーザ・ク

ライアント対の一部とすることができる。応答側IDciおよびIDcr NATフラグはそれぞれ独立にセットすることができる。両者とも、接続定義に外部初期設定モードがある場合にのみ適用される。

【0023】すべての場合において、NATフラグが「オン」の場合、接続定義において対応する細分度値は「s」(スカラー)でなければならない。

【0024】図2を参照すると、VEN NAT IPプールが各ネットワーク事例にどのように関係するかが図示されている。線34および36は、インターネット40上のゲートウェイ(Gw)42、44、および46間のIP Sec接続を表す。タイプaおよびc用のNATプール52、54に各リモートID(ゲートウェイ42、44、46)が独立して関連づけられている。タイプdのVEN NATには、VEN NATゲートウェイ42が所有するグローバルIPアドレスのために単一のプール50を定義することができる。この例では、3つの内部ネットワーク56、58、および60すべてが同じ10.*.*アドレス空間を使用する。これによって、VEN NATの初期値とモチベー

シオンが与えられる。これらの内部ネットワーク56、58、60間のIP Secトンネル(接続とも呼ぶ)は、それらを結合する論理的効果を持つ。これは一般には、アドレス競合なしに行うことができない。VEN NATは、ゲートウェイ(Gw)42がそれぞれ、内部ネットワーク60および58上のゲートウェイGw Q44およびGw Y46の背後のホストと取引する必要があるときに、ゲートウェイ(Gw)42に生じる問題を解決する。

【0025】ステップ22で、ユーザはVEN NAT機能の排他的使用のために使用可能な(プール50、52、および54内の)1組のIPアドレスを定義する。各プールは、IPアドレスの範囲として定義可能であることが好ましく、当然ながらリモートIDおよびローカルIDのIP Secポリシー・データベース・エンティティに関連づけられる。すなわち、各リモートID DB項目および各ローカルID DB項目ごとに、ユーザは任意選択により2つのIPアドレスを指定することができる。

【0026】表2を参照すると、異なるプールをモチベートする各種類のVEN NATの様々な意味が記載されている。1リモートIDまたはローカルID単位について指定しているが、プールはIPアドレスの3つの別個のグループとして管理することができる。これにより、ユーザはたとえば複数のリモートIDについて同じ範囲を指定することができる。文字a、c、およびdは、VEN NATタイプ(表1)に対応する。「lr?」欄は、(グローバルにルーティング可能と区別して)ローカルでルーティング可能であることを意味する。

【表2】

表2：IP Sec NAT プール（2の1）

IP Sec NAT プール	プールの目的	有効生成送出 NAT 規則	lr?
a. 「L」接続、IDcl（送出時の IP アドレスの送信元）を交換する。	<p>1. 自身の IP アドレスをリモート GW およびホストから隠蔽する（従来型 NAT と同じモチベーション）。</p> <p>2. リモート GW およびそのネットワークとの IP アドレス競合（VPN によって生じる可能性のある新たな問題）を回避する。</p> <p>したがって、プールを各リモート ID に関連づけることができる。</p>	「MAP srcIP TO<プールからの値>」。ユーザ・クライアント対、「ローカル・クライアント ID」から入手した NAT srcIP。	可

【0027】

【表3】

表2：IP Sec NAT プール（2の2）

IP Sec NAT プール	プールの目的	有効生成送出 NAT 規則	lr?
c. 「R」接続、IDcl（到着時のソース IP アドレス）を交換する。	<p>リモート GW およびそのネットワークとの IP アドレス競合（VPN によって生じる可能性のある新たな問題）を回避する。</p> <p>したがって、プールを各リモート ID に関連づけることができる。</p>	「MAP destIP TO<プールからの値>」。ISAKMP IDcl から入手した NAT destIP。	可
d. 「R」接続、IDcr（到着時の宛先 IP アドレス）を交換する。	<p>1. 単一の外部のグローバルにルーティング可能な IP アドレスから一種の負荷分散をサーバのセットに供給する。</p> <p>2. 自身の IP アドレスを外部アドレスの背後に隠蔽する。</p> <p>したがって、プールをグローバルにルーティング可能な IP アドレス（IDcr）に関連づけることができる。</p>	「MAP srcIP TO<プールからの値>」。ISAKMP IDcr から入手した NAT srcIP。	可

【0028】ステップ24で、開始側モード接続が開始される。開始側モード接続を開始するとき、接続マネージャはローカル・クライアントIDを交換すべきか否かを調べる。交換する場合、接続マネージャは、データベース内のリモートIDに関連づけられたNATプール、たとえば52から使用可能なIPアドレスを探す。接続マネージャは、使用可能であるか否かを以下のようにして判断す

50

る。接続マネージャは、いずれかのaタイプ・プール（表1参照）から、何らかのアクティブ接続（状態：開始、実行、または停止）で使用されたIPアドレスの単一の（接続マネージャは1システムについて1回実行されるためシステム規模で）リストを維持する。使用済みリストにないプール内の最初のIPアドレスを選択して使用済みリストに加える。使用可能なIPアドレスが見つから

13

ない場合、接続は開始されず、適切なエラー・メッセージ（および場合によってはOP NAV GUIへの戻りコード）が生成される。ポリシー・データベースは、IPアドレスが使用中であることを示すために更新されず、これは接続マネージャが、そのアクティブ接続のセットのみに基づいて動的に判断する。

【0029】接続マネージャからISAKMPに送られる開始メッセージ（msg）は、プールから選択されたNAT rhs IPアドレスを有することになる。このNAT rhs IPアドレスはSA対に加えられ、このSA対はISAKMPから返されたSA対によって完成される。接続マネージャは接続をIPSecにロードする。

【0030】IPSecはこの2つのSAのためにNAT規則を生成する。送出時、NATはフィルタリングの後、IPSecの前に行われ、到着時にはNATはIPSecの後（およびフィルタリングの前）に行われる。この場合、NATはIPSec接続のローカル・エンドをラッピングする。

【0031】図3および図4を参照すると、本発明によるVEN NATタイプを示す後の各図の背景および対照として、従来型NAT機能が図示されている。

【0032】図3を参照すると、静的NATはNATの最も単純な形態である。両方の従来型NATタイプは、ユーザがOP NAT GUIを介して対応するNAT規則ステートメントを作成することによって明示的に設定される。これは、実際のNAT規則またはステートメントがシステムによって生成されるIPSec NATとは異なる。MAPステートメント<MAP lhs TO rhs>とHIDEステートメント<HIDE ip addr set BEHIND rhs>がそのようなステートメントである。

【0033】再び図3を参照すると、到着処理時に、送信元（src）ip 7 0がMAP lhs TO rhsステートメント中のlhs 7 2と一致する場合、src ip 7 0はrhs 7 6に変換される。送出処理時、宛先（dst）ip 7 4がrhs 7 6と一致する場合、宛先ip 7 4がlhs 7 2に変換される。

【0034】図4を参照すると、マスカレードNAT（ネットワーク・アドレスおよびポート変換（NAPT）とも呼ぶ）がHIDEステートメントsupraを使用し、それ自体のポート・プール118（UDP、TCP）を使用して多対1アドレス変換を行い、到着トラフィックの変換方法を記憶している。静的NAT（図3）とは異なり、マスカレードNAT会話<CONVERSATION src ip, src port, rhs ip, rhs port, ...>は、内部（lhs）アドレスによってのみ開始することができる。VEN NAT（本発明の好ましい実施形態を識別するために使用する名称）は、後述するように、ポート変換を含まないという点で静的NATに近い。

【0035】さらに図4を参照すると、送出データグラムの処理において、ステップ<1>で送信元ipアドレス90がHIDEステートメントのipアドレス・セット92にある場合、ポート・プール118内の適切なプールから、ステップ<2>でsrc ip 90をCONVERSATIONフィールド94にコピーし、ステップ<3>で送信元ポート9

14

8をフィールド96にコピーし、ステップ<4>でrhs 104をフィールド100にコピーし、ステップ<5>でrhsポートをフィールド102にコピーすることによってCONVERSATIONがセット・アップされる。次に、ステップ<6>で、送信元ip 90がrhs 104に変換され、ステップ<7>で送信元ポートと98がrhsポート102に変更される。到着データグラムの処理において、ステップ<8>で宛先ipアドレス106および宛先ポート108がCONVERSATIONフィールドrhs ip 100およびrhsポート102とそれぞれ一致する場合、ステップ<9>で宛先ipアドレス106がCONVERSATION送信元ipアドレス94に変換され、ステップ<10>で宛先ポート108がCONVERSATION送信元ポート96に変換される。

【0036】NATによって処理される特殊な状況の中には、本発明の対象ではないため、図示されていないものもある。これには、FTPまたはICMP（両者とも変換されるIPアドレスを含む）によって生じる特殊な状況の処理が含まれる。チェックサム再計算を行う。マスカレードNATコードでは、会話があった後は、後のデータグラムを元の（性急な）HIDE規則ではなくその会話と突き合わせ、ポート・プールの管理し、会話のタイミングをとって終了し、ポートをマップする。VEN NATが、（周知のFTP PORTコマンドおよびそれに付随する問題を含めて）ICMPおよびFTPをサポートすることは本発明の特別な利点である。

【0037】図5を参照すると、VEN NATタイプ「a」の本発明の好ましい実施形態が図示されている。VEN NATのタイプ「a」では、開始側モード会話のためにIDciが変換される。システム生成の暗黙的NAT規則128<MAP lhs TO rhs>がロードされた後、これは静的NATとして機能する。この作業を行う鍵は、ISAKMPによってネゴシエーションされたセキュリティ・アソシエーションが暗黙的MAP130 rhs 138を使用することである。したがって、SAとVEN NATが同期化される。

【0038】さらに図5を参照すると、ローカルで開始された会話のために、ステップ<-2>で、NATが要求されたためにローカルで開始された会話について、ローカル・クライアントID122をlhs 126にコピーすることによって暗黙的MAP規則128を作成し、適切なプールからipアドレス120を入手してrhs 124にコピーする。ステップ<0>で、rhs 124を使用してISAKMPネゴシエーションが完了した後、暗黙的MAP規則130をロードする。送出処理の場合、ステップ<1>でsrc ip 132がlhs 136と一致する場合、ステップ<2>でsrc ipがrhs 138に変換される。到着処理の場合、ステップ<3>でdest ipアドレス140がrhs 138と一致する場合、ステップ<4>で宛先ip 140がlhs 136に変換される。

【0039】ステップ26で、応答側モード接続が開始される。その際、ISAKMP機能が現在設定されているポ

10

20

30

40

50

15

リシーに基づいてSAをネゴシエーションする。完了すると、それらのSAがn個のSA対から成るSAの集合としてSA接続マネージャに送られる。

【0040】接続マネージャは、ISAKMPから開始メッセージ(msg)を受け取ると、データベース内の接続定義を調べ、IDcrおよびIDci NATフラグを検査する。NATリモート・フラグが「オン」の場合、リモートIDに関連づけられた適切なNATプールからIPアドレスを入手する。NATローカル・フラグが「オン」の場合、IDcrに関連づけられたプールからIPアドレスを入手する(グローバル・

アドレス)。図6および図7に、VEN NATタイプ「c」および「d」が図示されている。

【0041】リモートIPプールからのIPアドレスの可用性の管理は、(タイプ「a」VEN NATの場合と同様に)接続マネージャがそのアクティブ接続のセットに基づいて行う。接続マネージャは、IDcrプールの可用性も扱い、それによって負荷バランシングが可能になる。IDcrはIDcrをネットワーク・アドレス変換するためのIPアドレスのセットである。以下の2つの基本手法がある。すなわち、(1)開始のたびにプールを最初の項目から探索するか、または(2)開始のたびにプールを最後に使用されたIPから探索する手法である。

【0042】IPSecへのロードは、前述の開始側モードの事例と同様に行われる。Rタイプの接続トラフィック(接続名中で、連続するバイトの最初のバイトが「R」である)を処理する場合、各到着および送出パケット(送信元および宛先)について2つのアドレス変換が行われることがある。

【0043】図6を参照すると、VEN NATタイプ「c」が実行されて、応答側モード会話のIDciが以下のように変換される。ステップ<2>で、リモートで開始された会話について、初めにNATが要求されたために、暗黙的MAP規則158<MAP lhs TORhs>が作成され、IDci152がrhs154にコピーされる。ステップ<1>で、適切なプール150からipアドレスを入手してlhs156にコピーする。ステップ<0>で、rhs154を使用してISAKMPネゴシエーションが完了した後で、暗黙的規則160がロードされる。到着データグラムを処理するとき、ステップ<1>でsrcip172がrhs168と一致する場合、ステップ<2>で送信元ip172がlhs166に変換される。送出データグラムを処理するとき、ステップ<3>で宛先164がlhs166と一致する場合、ステップ<4>で宛先ip164がrhs168に変換される。

【0044】図7を参照すると、VEN NATタイプ「d」が実行され、以下のように応答側モード会話のためにIDcrを変換する。ステップ<2>で、初めに、リモートで開始された会話について、NATが要求されたため、暗黙的MAP規則188が作成され、IDcr182がrhs184にコピーされる。ステップ<1>で、適切なアドレス

16

・プール180からipアドレスを入手してlhs186にコピーする。ステップ<0>で、rhs184を使用してISAKMPネゴシエーションが完了した後、暗黙的MAP規則190がロードされる。到着データグラムを処理するとき、ステップ<1>で宛先ip200がrhs198と一致する場合、ステップ<2>で宛先ip200がlhs196に変換される。送出データグラムを処理するときは、ステップ<3>で送信元ip192がlhs196と一致する場合、ステップ<4>で送信元ip192がrhs198に変換される。

【0045】ステップ28で、接続マネージャはSA対の更新を入手すると、既存のSA対内のNAT IPアドレスをその新しいSA対にコピーする。

【0046】ステップ30で、接続を終了するとき、接続マネージャはその接続に関連づけられたNAT IPアドレスを解放する(使用可能にする)。接続マネージャによって維持されている該当するリストからNAT IPアドレスが除去される。

【0047】

【発明の効果】本発明の利点は、ネットワーク・アドレス変換(NAT)とIPセキュリティ(IPSec)の両方を並列して実施する改良されたシステムおよび方法が提供されることである。

【0048】本発明の他の利点は、仮想プライベート・ネットワーク(VEN)の使用に固有のIPアドレス競合の可能性の増大を解決するシステムおよび方法が提供されることである。

【0049】本発明の他の利点は、(高くつく代替策である)ドメインの再アドレス指定の必要なしに、VENの使用を可能にするシステムおよび方法が提供されることである。

【0050】本発明の他の利点は、ドメイン・ホストに変更を加える必要なしに、完全にIPSecゲートウェイだけで実現されるVEN NATのためのシステムおよび方法が提供されることである。

【0051】本発明の他の利点は、各接続ドメインにおいてルーティングにまったく変更を加える必要がないか、またはわずかな変更しか必要としない、VEN NATのためのシステムおよび方法が提供されることである。

【0052】本発明の他の利点は、設定が単純なVEN NATのためのシステムおよび方法が提供されることである。

【0053】本発明の他の目的は、VENによって生じるアドレス衝突問題の解決策が提供されることである。

【0054】代替実施形態

本明細書では、例示のために本発明の特定の実施形態について説明したが、本発明の主旨および範囲から逸脱することなく、様々な変更を加えることができる。具体的には、本発明の方法に従って今の動作を制御するため、または本発明のシステムによりその構成要素を構成する

ために、機械による読取り可能な信号を記憶する固体または流体の伝送媒体、磁気または光配線、テープまたはディスクなどのプログラム記憶装置またはメモリ装置を提供することも、本発明の範囲に含まれる。

【0055】まとめとして、本発明の構成に関して以下の事項を開示する。

【0056】(1) ネットワーク・アドレス変換 (NAT) を IP Sec 処理と統合する IP Sec に基づく仮想プライベート・ネットワーク (VPN) を動作させる方法であって、 NAT IP アドレス・プールを設定するステップと、前記 NAT IP アドレス・プールを使用するために VPN 接続を設定するステップと、前記 NAT IP アドレス・プールから特定の IP アドレスを入手し、前記特定の IP アドレスを前記 VPN 接続に割り振るステップと、前記 VPN 接続を開始するステップと、オペレーティング・システム・カーネルに前記 VPN 接続のためのセキュリティ・アソシエーションと接続フィルタをロードするステップと、前記 VPN 接続のための IP データグラムを処理するステップと、前記 IP データグラムに VPN NAT を適用するステップとを含む方法。

(2) 前記 VPN 接続が送出処理のために設定され、前記適用ステップが送出送信元 IP のネットワーク・アドレス変換を含む、上記 (1) に記載の方法。

(3) 前記 VPN 接続が到着処理の何らかの組合せのために設定され、前記適用ステップが到着送信元 IP のネットワーク・アドレス変換または到着宛先 IP のネットワーク・アドレス変換を選択的に含む、上記 (1) に記載の方法。

(4) 手動鍵 IP Sec 接続のための NAT と IP Sec との統合のために、接続鍵を手動で設定するステップをさらに含む、上記 (1) に記載の方法。

(5) 動的鍵 (たとえば IKE) IP Sec 接続のための NAT と IP Sec との統合のために、VPN 接続の鍵を自動的に入手するように前記 VPN 接続を設定するステップをさらに含む、上記 (1) に記載の方法。

(6) NAT を IKE によって動的にネゴシエーションされた IP Sec セキュリティ・アソシエーションと統合するために、前記開始ステップが、前記 NAT プールからの前記 IP アドレスを含む IKE のためにメッセージを作成するステップをさらに含み、動的にネゴシエーションされた鍵を入手するように IKE を動作させるステップをさらに含む、上記 (1) に記載の方法。

(7) 前記動的に入手した鍵を前記 NAT プール IP アドレスと結合するステップをさらに含み、前記ロードするステップが前記結果をセキュリティ・アソシエーションとして前記オペレーティング・システム・カーネルにロードするステップを含む、上記 (6) に記載の方法。

(8) VPN 接続および VPN ポリシーの定義および設定を直接使用する NAT の定義および設定を可能にする方法であって、 VPN NAT タイプ a 送出送信元 IP NAT と VPN NAT タイ

プ c 到着送信元 IP NAT と VPN NAT タイプ d 到着宛先 IP NAT の 3 つのタイプの VPN NAT のうちの各タイプのためのポリシー・データベースにおける肯定/否定の決定によって VPN NAT のための要件を設定するステップと、前記各 VPN NAT タイプの前記肯定/否定の決定に回答してリモート IP アドレス・プールまたはサーバ IP アドレス・プールを選択的に設定するステップとを含む方法。

(9) VPN 接続が必要になる各リモート・アドレスのために固有な前記リモート IP アドレス・プールを設定するステップであって、前記リモート IP アドレス・プールがリモート IP によって鍵づけされるステップをさらに含む、上記 (8) に記載の方法。

(10) 設定されるシステムのために 1 回前記サーバ IP アドレス・プールを設定するステップをさらに含む、上記 (8) に記載の方法。

(11) オペレーティング・システム・カーネルで VPN NAT 活動が行われるにつれて VPN NAT 活動の顧客追跡を実現する方法であって、 VPN 接続設定に回答して、ジャーナル・レコードを生成するステップと、 VPN 接続を介して処理された各データグラムの新しいレコードによって前記ジャーナル・レコードを更新するステップと、顧客が前記ジャーナル・レコードを管理することができるようにするステップとを含む方法。

(12) VPN NAT アドレス・プールをゲートウェイに関連づけることができるようにし、それによってサーバ負荷バランスをとることができるようにする方法であって、設定するシステム用にサーバ NAT IP アドレス・プールを設定するステップと、前記サーバ NAT IP アドレス・プールにグローバルにルーティング可能な特定の IP アドレスを格納するステップと、前記サーバ NAT IP アドレス・プールを使用するように VPN 接続を設定するステップと、前記サーバ NAT IP アドレス・プール内のアドレスの数に回答して、並列 VPN 接続の合計量を管理するステップとを含む方法。

(13) NAT アドレスの可用性に基づいてシステムのための VPN 接続の合計数を制御する方法であって、 IP アドレスの共通セットを使用してリモート IP アドレス・プール全体を設定するステップと、前記リモート・アドレス・プール全体にわたって設定された前記 IP アドレスの数に回答して、並列してアクティブである VPN 接続の成功裏の開始を制限するステップとを含む方法。

(14) 選択された ICMP データグラムに対してネットワーク・アドレス変換を実行する方法であって、選択されたタイプの ICMP タイプ・パケットを検出するステップと、前記選択されたタイプに回答して、 ICMP データを含む前記データグラム全体に対してネットワーク・アドレス変換機能を実行するステップとを含む方法。

(15) 選択された FTP データグラムに対してネットワーク・アドレス変換を実行する方法であって、 FTP PORT コマンドまたは PASV FTP コマンドの発生を検出するステ

19

ップと、前記コマンドに応答して、前記FTPデータおよびヘッダに対してネットワーク・アドレス変換を実行するステップとを含む方法。

(16) ネットワーク・アドレス変換(NAT)をIP Sec処理と統合するIP Secに基づく仮想プライベート・ネットワーク(VEN)を動作させるシステムであって、NAT IPアドレス・プールを設定する手段と、前記NAT IPアドレス・プールを使用するためにVEN接続を設定する手段と、前記NAT IPアドレス・プールから特定のIPアドレスを入手し、前記特定のIPアドレスを前記VEN接続に割り振る手段と、前記VEN接続を開始する手段と、オペレーティング・システム・カーネルに前記VEN接続のためのセキュリティ・アソシエーションと接続フィルタをロードする手段と、前記VEN接続のためのIPデータグラムを処理する手段と、前記IPデータグラムにVEN NATを適用する手段とを含むシステム。

(17) VEN接続およびVENポリシーの定義および設定を直接使用するNATの定義および設定のためのシステムであって、VEN NATタイプa 送出送信元IP NATとVEN NATタイプc 到着送信元IP NATとVEN NATタイプd 到着宛先IP NATの3つのタイプのVEN NATのうちの各タイプのための肯定/否定の決定によってVEN NATのための要件を設定するポリシー・データベースと、前記各VEN NATタイプの前記肯定/否定の決定に回答して選択的に設定されるリモートIPアドレス・プールまたはサーバIPアドレス・プールとを含むシステム。

(18) VEN NATアドレス・プールをゲートウェイに関連づけることができるようにし、それによってサーバ負荷バランスをとることができるようにするシステムであって、設定される所与のシステム用に設定されたサーバNAT IPアドレス・プールと、グローバルにルーティング可能な特定のIPアドレスを格納する前記サーバNAT IPアドレス・プールと、前記サーバNAT IPアドレス・プールを使用するように設定されたVEN接続と、前記サーバNAT IPアドレス・プール内のアドレスの数に回答して、並列VEN接続の合計量を管理する接続コントローラとを含むシステム。

(19) ネットワーク・アドレス変換(NAT)をIP Sec処理と統合するIP Secに基づく仮想プライベート・ネットワーク(VEN)を動作させる方法ステップを実行するように機械によって実行可能な命令から成るプログラムを有形に実施する、機械による読取り可能なプログラム記憶装置であって、前記方法ステップは、NAT IPアドレス・プールを設定するステップと、前記NAT IPアドレス・プールを使用するためにVEN接続を設定するステップと、前記NAT IPアドレス・プールから特定のIPアドレスを入手し、前記特定のIPアドレスを前記VENに割り振るステップと、前記VEN接続を開始するステップと、オペレーティング・システム・カーネルに前記VEN接続のためのセキュリティ・アソシエーションと接続フィルタを

20

ロードするステップと、前記VEN接続のためのIPデータグラムを処理するステップと、前記IPデータグラムにVEN NATを適用するステップとを含むプログラム記憶装置。

(20) ネットワーク・アドレス変換(NAT)をIP Sec処理と統合するIP Secに基づく仮想プライベート・ネットワーク(VEN)を動作させる、その中に実施されたコンピュータ可読プログラム・コード手段を有するコンピュータ使用可能媒体を含む製造品であって、前記製造品内の前記コンピュータ可読プログラム手段は、コンピュータにNAT IPアドレス・プールの設定を行わせるコンピュータ可読プログラム・コード手段と、コンピュータに前記NAT IPアドレス・プールを使用するようにVEN接続の設定を行わせるコンピュータ可読プログラム・コード手段と、コンピュータに、前記NAT IPアドレス・プールから特定のIPアドレスを入手させ、前記特定のIPアドレスを前記VEN接続に割り振らせるコンピュータ可読プログラム・コード手段と、コンピュータに前記VEN接続を開始させるコンピュータ可読プログラム・コード手段と、コンピュータに、前記VEN接続のためのセキュリティ・アソシエーションと接続フィルタとをオペレーティング・システム・カーネルにロードさせるコンピュータ可読プログラム・コード手段と、コンピュータに前記VEN接続のためのIPデータグラムを処理させるコンピュータ可読プログラム・コード手段と、コンピュータに前記IPデータグラムへのVEN NATの適用を行わせるコンピュータ可読プログラム・コード手段とを含む製造品。

(21) ネットワーク・アドレス変換(NAT)を使用して仮想プライベート・ネットワークにIPセキュリティを設ける方法であって、NAT規則を動的に生成し、前記NAT規則を、手動または動的に生成された(IKE)セキュリティ・アソシエーションに関連づけるステップと、その後で、前記セキュリティ・アソシエーションを使用するIPセキュリティを開始するステップと、その次に、送出データグラムおよび到着データグラムに対してIP Secが実行されるときに、VEN NATタイプa 送出送信元IP NAT、VEN NATタイプc 到着送信元IP NAT、およびVEN NATタイプd 到着宛先IP NATのうちの1つまたは複数のタイプを選択的に実行するステップとを含む方法。

【図面の簡単な説明】

【図1】本発明の好ましい実施形態のVEN NAT方法を示す流れ図である。

【図2】典型的なIP Secの事例とそれに付随するVEN NATプールを示す図である。

【図3】最も単純な従来のNATである静的NATを示す図である。

【図4】従来のNATの1タイプであるマスカレードNATを示す図である。

【図5】VEN NAT、タイプa：開始側モード会話のために変換されたIDciを示す図である。

【図6】VPN NAT、タイプc：応答側モード会話のために変換されたIDciを示す図である。

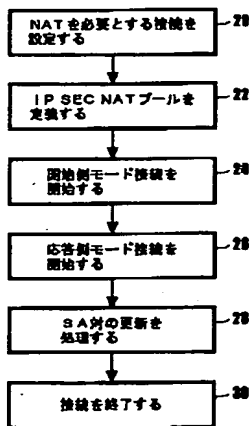
【図7】VPN NAT、タイプd：応答側モード会話のために変換されたIDcrを示す図である。

【符号の説明】

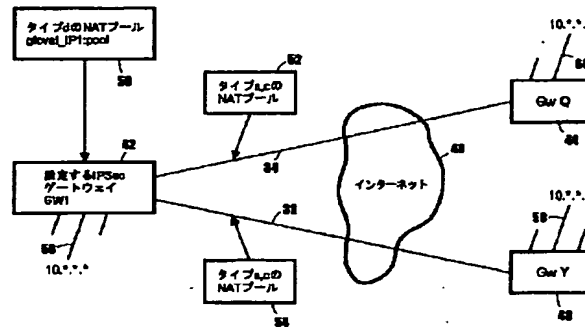
40 インターネット
42 ゲートウェイ
44 ゲートウェイ
46 ゲートウェイ
50 タイプdのNATプール
52 タイプaのNATプール
54 タイプcのNATプール
56 内部ネットワーク
58 内部ネットワーク
60 内部ネットワーク
120 IPアドレス・プール
122 クライアントID
128 暗黙的NAT規則

130 暗黙的MAP
140 宛先IP
142 送信元IP
132 送信元IP
134 宛先IP
150 IPアドレス・プール
160 暗黙的規則
162 送信元IP
164 宛先IP
170 宛先IP
172 送信元IP
180 IPアドレス・プール
188 暗黙的MAP規則
190 暗黙的MAP規則
192 送信元IP
194 宛先IP
200 宛先IP
202 送信元IP

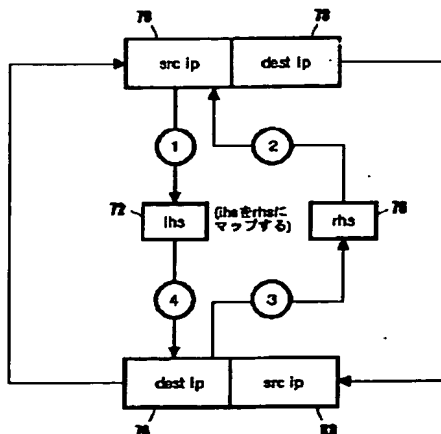
【図1】



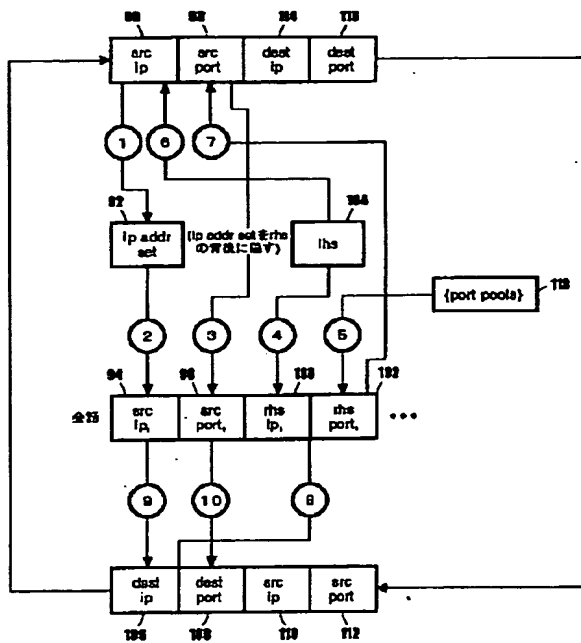
【図2】



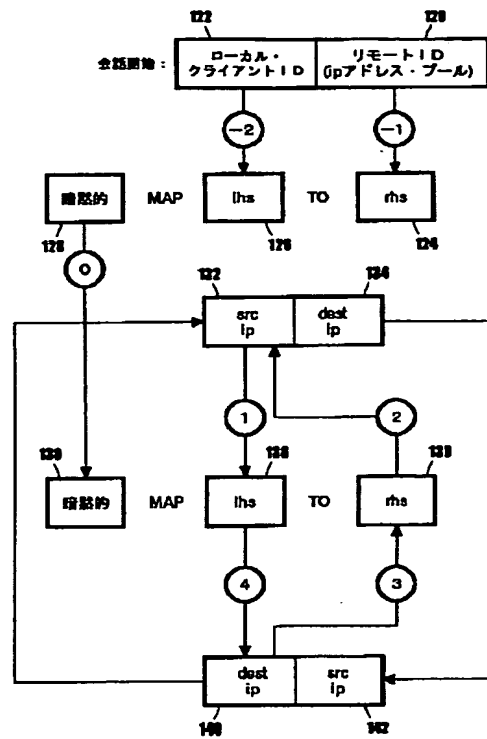
【図3】



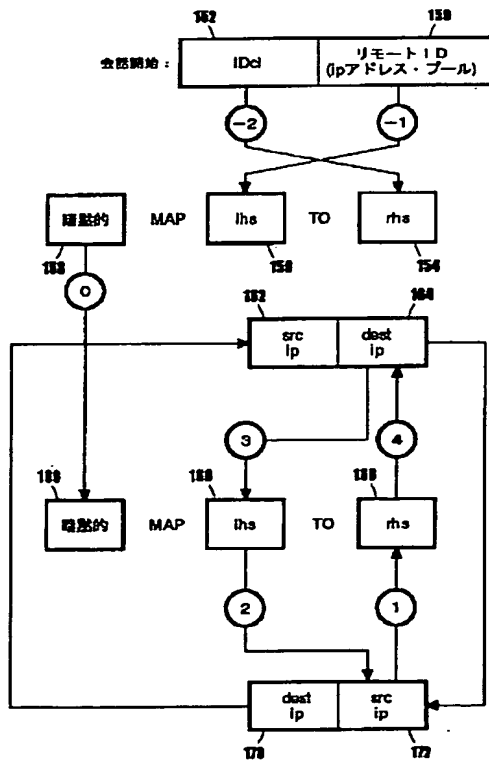
【图 4】



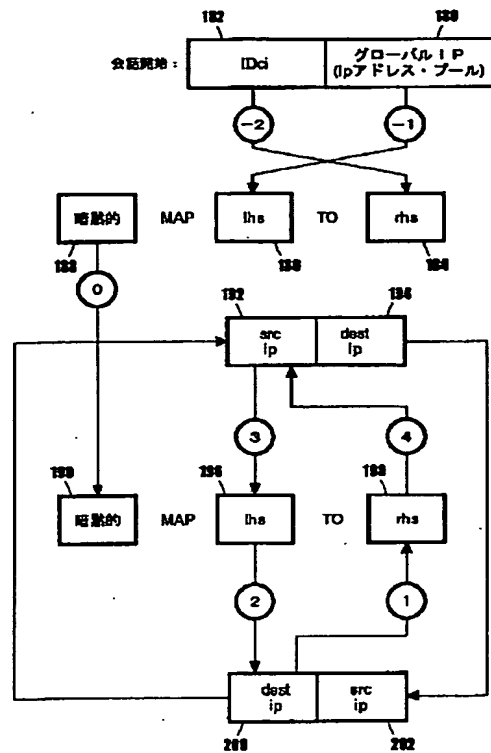
【图5】



【図6】



【図7】



フロントページの続き

(72)発明者 フランクリン・エイ・グルーバー
アメリカ合衆国13850 ニューヨーク州
ベストル デナル・ウェイ413

(56)参考文献 特開2001-352344 (J P, A)
P. Srisuresh, Security model with Tunnel-mode IPsec for NAT Domains, RFC 2709, 1999年10月31日

(58)調査した分野(Int.Cl.⁷, DB名)
H04L 9/00
H04L 12/46
H04L 12/56
H04L 12/66
WPI (DIALOG)